UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/751,829	12/29/2000	Shlomi Harif	AUS9000888US1	8494

35617 7590 01/31/2005

DAFFER MCDANEIL LLP
P.O. BOX 684908
AUSTIN, TX 78768

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/751,829	**Applicant(s)** HARIF, SHLOMI	
	Examin r Matthew T Henning	**Art Unit** 2131	

-- Th MAILING DATE of this communication appears on th cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 27 August 2004.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5,7-11,13-17,19,20,22-25,27-36,40,44-46,52,57 and 58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5,7-11,13-17,19,20,22-25,27-36,40,44-46,52,57 and 58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 27 August 2004 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

This action is in response to the communication filed on 8/27/2004.

DETAILED ACTION

1. Claims 4, 6, 12, 18, 21, 26, 37-39, 41-43, 47-51, 53-56, and 59-62 have been cancelled.

2. Claims 1-3, 5, 7-11, 13-17, 19-20, 22-25, 27-36, 40, 44-46, 52, and 57-58 have been examined.

3. All rejections and objections not specifically set forth below have been withdrawn.

Title

4. The title of the invention is acceptable.

Priority

5. The application has been filed under Title 35 U.S.C §119, claiming priority to Provisional application 60/230,107, filed September 5, 2000.

6. The effective filing date for the subject matter defined in the pending claims in this application is September 5, 2000.

Information Disclosure Statement

7. The information disclosure statement (IDS) submitted on September 20, 2001 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Drawings

8. The drawings were received on 8/27/2004. These drawings are acceptable.

Specification

9. The abstract of the disclosure is objected to because

Line 2: The phrase "are provided" can be implied and therefore must be removed.

Correction is required. See MPEP § 608.01(b).

Claim Objections

10. Claims 29-32 and 44-46 are objected to under 37 CFR 1.75(a), as being of improper dependent form for particularly point out and distinctly claim the subject matter which the applicant regards as the invention. Claims 29-32 depend on the cancelled claim 26, and claims 44-46 depend on the cancelled claim 43. Therefore, it is not possible to determine the scope of these claims. For purposes of applying prior art, the examiner will presume that 29-31 were meant to depend on claim 25, and claim 44 was meant to depend on claim 40.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> *A person shall be entitled to a patent unless –*
>
> *(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.*

12. Claims 1, 4-7, 12 rejected under 35 U.S.C. 102(b) as being anticipated by Schuermann (U.S. Patent 5,552,789) hereinafter referred to as Schuermann.

13. Claim 1 recites a first computational device containing tags and associated rules sets for controlling operational privileges. Schuermann disclosed a controller (computational device) identifying transponders based on the encoded data (tag) stored within each transponder (See Schuermann Col. 8 Paragraph 2) and using this information received from the transmitter to adjust the operational parameters of the vehicle (See Schuermann Col. 8 Lines 4-11 and Lines 16-18). Schuermann also disclosed that these settings were previously stored in the controller (See Schuermann Col. 8 Lines 64-67).

Claim 1 further recites a second computational device for programming an access device with an identification tag after authorization from the first computational device. Schuermann disclosed a writer, controlled by the controller (See Schuermann Figure 1 Element 10), for writing to the transponders (See Schuermann Col. 5 Lines 44-47). Because the data stored on the transponder identifies the transponder to the controller (See Schuermann Col. 8 Paragraph 2) it is inherent that the data written to the transponder is used for identification purposes and is therefore a tag.

14. Claims 4 and 5 recite a third computational device for writing the tags to the access device and for re-authenticating the access device upon authorization from the first computational device. Schuermann disclosed an interrogator controlled by the controller for reading from and writing to the transponder (See Schuermann Col. 3 Paragraph 5). Because the data stored on the transponder identifies the transponder to the controller (See Schuermann Col. 8 Paragraph 2) it is inherent that the data written to the transponder is used for identification purposes and is therefore a tag.

Schuermann further disclosed the interrogator re-authenticating the transponders on a regular basis (See Schuermann Col. 8 Paragraph 4). Schuermann also disclosed that the interrogator may be satellite to the controller, but still controlled by the controller (See Schuermann Claim 19).

15. Regarding claim 6, because all of the elements of the system disclosed by the combination of Schuermann communicated between each other, it was inherent that some form of a network connected them.

16. Claim 12 recites the network comprising the Internet. Schuermann disclosed communicating with tollbooths regarding credit authorization information (See Schuermann Col. 7 Paragraphs 3-4), which constitutes the Internet.

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

18. Claims 1-3, and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ohashi et al. (US Patent Number 5,761,309) hereinafter referred to as Ohashi.

19. Regarding claim 1, Ohashi disclosed A network system for providing a level of operation privileges to a user (See Ohashi Abstract), the system comprising: a first computational device (See Ohashi Fig. 1 Element 15 Slave AuC) comprising an identification tag (c_addr) and associated rule set (License), wherein each identification tag and rule set pair establishes a level of operation privileges (Permission information) to the user (See Ohashi Fig. 4 and Col. 9 Paragraph 2 and Col. 6 Paragraph 4); a second computational device (See Ohashi Fig. 1 Client Terminal/Card reader/write) adapted to program an access device (See Ohashi Fig. 1 Smart Card) with at least one of the identification tags upon authorization from the first computational device (See Ohashi Fig. 4 and Col. 9 Paragraphs 3-4 wherein the authorization from the Slave AuC is inherent in the sending of the License, and the Terminal causes the License to be stored in the card); a third computational device adapted to program the access device with at least one of the identification tags upon authorization from the first computational device (See Ohashi Col. 5 Paragraph 2 wherein there are a plurality of client terminals); and wherein the first, second, and third computational devices are interconnected via the Internet (See Ohashi Fig. 1 Network and Col. 17 Paragraph 2 wherein the network is the Internet). However, Ohashi failed to disclose the Slave AuC containing a plurality of Licenses.

Ohashi did hint at this, however, by disclosing that there were a plurality of users, and Application servers (See Ohashi Col. 5 Paragraph 2 and Col. 11 Paragraph 9). This suggests that multiple Licenses would have been present on the Slave AuC.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the suggestions of Ohashi in the authentication system by having the Slave AuC contain more than one license. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide multiple users with access to the application servers.

It also would have been obvious to the ordinary person skilled in the art at the time of invention to employ the suggestions of Ohashi in the authentication system by having the client terminal contain more than one license. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow a user to access more than one application server at any given time.

20. Regarding Claim 2, Ohashi disclosed that the second computational device was further adapted to program an authentication device (Application Server) with a plurality of the identification tags and associated rule sets upon authorization from the first computational device (See Ohashi Fig. 5 and Col. 9 Paragraph 5 wherein it was inherent that authorization was given when the Slave AuC sent the License to the client terminal).

21. Regarding claim 3, Ohashi disclosed that the authentication device was adapted to interface with the access device and provide the corresponding level of operation privileges to the user if the identification tag programmed in the access device matches with at least one of the identification tags programmed on the authentication device (See Ohashi Fig. 5 and Col 9 Paragraph 6 – Col. 10 Paragraph 5).

22. Regarding Claim 5, Ohashi disclosed the access device is adapted to be periodically re-authenticated by the third computational device upon authorization from the first computational device (See Ohashi Col. 5 Paragraph 8 – Col. 6 Paragraph 2 wherein the user is re-authenticated each time the card is inserted into a new terminal).

23. Claims 7-11, 13-17, 19-20, 22-24, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schuermann (US Patent number 5,552,789), and further in view of Kolls (US Patent Number 6,389,337).

24. Regarding claim 7, Schuermann disclosed an encoding device for programming a tag into an access device upon authorization from a central authority. Schuermann disclosed a central authority (a controller) (See Schuermann Col. 2 Paragraph 4). Schuermann further disclosed a writer, controlled by the controller (See Schuermann Figure 1 Element 10), for writing to the transponders (See Schuermann Col. 5 Lines 44-47). Because the data stored on the transponder identifies the transponder to the controller (See Schuermann Col. 8 Paragraph 2) it is inherent that the data written to the transponder is used for identification purposes and is therefore a tag.

Because communications between the transponders and the controller were via radio frequency communication links (See Schuermann Col. 3 Paragraph 2), it was inherent that an encoding device was provided to encode the communications to the correct radio frequency prior to transmission. The TIRIS reader/writer disclosed by Schuermann (See Schuermann Col. 5 Paragraph 5) showed this RF encoding.

However, Schuermann failed to disclose the controller being connected to the Internet. Schuermann did, however, disclose the controller connecting to a Toll Booth for processing credit transactions (See Col. 7 Paragraph 4), but does not disclose how the toll booth processes the credit transactions.

Kolls teaches a system in which a Toll Booth automatically receives credit information from a vehicle and processes the information through the Internet (See Kolls Col. 7 Paragraph 8 and Col. 21 Paragraphs 4-8).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kolls in the authentication system of Schuermann by providing the Toll Booth with a connection to the Internet. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a means for processing the credit transactions through the tollbooth. In this combination, the controller would have been connected to the Internet during the processing of the toll transaction.

25. Claim 8 recites the encoding device programming an authentication device with the plurality of identification codes. Schuermann disclosed multiple transponders and the ability to identify each (See Schuermann Col. 8 Paragraph 2). Schuermann further disclosed the reader receiving information from the transponders, verifying the identity of the transponder using the received information, and then applying the corresponding initialization parameters from previously stored data (See Schuermann Col. 8 Paragraph 5). In order for the reader to verify the identity of the transponder and its corresponding parameters, it was necessary that the reader had access to the access codes and parameters. Therefore, they must have been stored in the reader.

Further, because the writer already had the task of writing the access codes to the transponder, and the reader (authentication device) needed the codes as well, it would have been obvious to the ordinary person skilled in the art to have the writer program the codes into the reader as well. This would have been obvious because the ordinary person skilled in the art would have been motivated to use the writer for all necessary writing as opposed to having multiple writers. Schuermann hinted at the idea of only having a single reader and writer by supplying a multiplexer for communicating with the transponders (See Schuermann Figure 1 Element 12).

26. Claim 9 recites the central authority maintaining and administering tags and associated rules sets for controlling operational privileges. Schuermann disclosed a controller (central authority) identifying transponders based on the encoded data (tag) stored within each transponder (See Schuermann Col. 8 Paragraph 2) and using this information received from the transmitter to adjust the operational parameters of the vehicle (See Schuermann Col. 8 Lines 4-11 and Lines 16-18). Schuermann also disclosed that these settings were previously stored in the controller (See Schuermann Col. 8 Lines 64-67).

27. Claim 10 recites that each identification tag and rule set pair establishes a level of operation privileges for the user (See rejection of claim 9 above).

28. Claim 11 recites the access device and the authentication device interfacing in order to provide the operational privileges if the access device provides a recognized tag. (See Schuermann Col. 8 Paragraph 5).

29. Claim 13 is rejected for the same reasons as claims 7, 8 and 10 above, and further because the controller was connected to the toll booth, and the toll booth was connected to the Internet, the controller was arranged in the Internet.

30. Claim 14 is rejected for the same reasons as claim 11 above.

31. Claim 15 is rejected for the same reasons as claim 7 above.

32. Claim 16 is rejected for the same reasons as claim 8 above.

33. Claim 17 rejected for the same reasons as claim 11 above.

34. Claims 19 and 20 are rejected for the same reasons as claims 7 and 8 above.

35. Claim 22 is rejected for the same reasons as claims 9 and 10 above.

36. Claim 23 is rejected for the same reasons as claim 11 above.

37. Regarding claim 24, Schuermann disclosed the TIRIS reader/writer re-authenticating the transponders on a regular basis, including the access device (Element 22) (See Schuermann Col. 8 Paragraph 4).

38. Claim 40 is rejected for the same reasons as claims 7-10 above and further because it is inherent that the data encoded in the transponders and the settings associated with them were established before the controller could use them as disclosed by Schuermann (See Schuermann Col. 8 Paragraphs 1-2). Schuermann disclosed an RF communication link between the controller and the transponder (See Schuermann Col. 8 Paragraph 3). Schuermann further disclosed establishing such a link, retrieving the access codes from the transponder (identification tag), verifying the codes, and applying previously stored pre-set requirements (See Schuermann Col. 8 Paragraph 5). It was inherent that the pre-set requirements were retrieved in order to apply them. Schuermann further disclosed that the vehicle performance limitations and the vehicle adjustments are uniquely associated with the key transponder (See Schuermann Col. 8 Paragraph 1). Schuermann disclosed that until a proper identification code is provided, the engine would not start (See Schuermann Col. 7 Paragraph 1). This falls within the scope of default operation privileges.

39. Claims 25, 27-36, 44-46, 52, and 57-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Schuermann and Kolls as applied to claim 7 above, and further in view of Treharne et al (U.S. Patent Number 5,416,471) hereinafter referred to as Treharne.

The combination of Schuermann and Kolls disclosed an access device adapted to store a programmed identification tag, wherein the access device is programmed upon authorization from a central authority connected to the network system (see rejection of claim 7 above); a vehicle comprising an authentication device adapted to store a plurality of programmed identification tags and associated rule sets, wherein the authentication device is programmed upon authorization from the central authority (See rejection of claim 8 above and Fig. 1 and 2 Element 10 wherein Schuermann clearly depicted the TIRIS reader and controller in a vehicle); wherein the central authority maintains and administers the plurality of identification tags and associated rule sets, and wherein each identification tag and rule set pair establishes a level of operation privileges to the user of the vehicle (See rejection of claims 9 and 10 above); and that until a proper identification code is provided, the engine would not start (See Schuermann Col. 7 Paragraph 1). However, Schuermann failed to disclose a method for bypassing the operational privileges of a key. Schuermann also failed to disclose a method for programming new keys for access to the system.

Treharne teaches that a spare vehicle key can be programmed into a security system by using a known key to provide authorization to program a new key (See Treharne Abstract). Treharne shows the steps of programming the new key into the system in Figure 3. The steps include authenticating a first key (See Figure 3 Step 54), inserting the new, un-programmed, key (See Figure 3 Step 60), reading the information on the new key (See Figure 3 Step 62), and then programming the new key into the system (See Figure 3 Step 66), at which point the key is able to open the lock.

It would have been obvious to the ordinary person skilled in the art to employ the teachings of Treharne in the invention of Schuermann in order to program new keys for authorization in the system. This would have been obvious because one of ordinary skill in the art would have been motivated to provide the vehicle owners with a simple method for granting new users, such as first time drivers, with access and operational privileges.

In this combination, the newly programmed key would have bypass its original operating parameters, and provided a dissimilar level of operation parameters.

Further in this combination, because the tag was written to the transponder, and the controller identified the transponder by this tag, it was inherent that the new tag granting privileges replaced the old tag on the transponder. Therefore, access to the old tag was disabled.

40. Claim 27 is rejected for the same reasons as claim 7 above.

41. Claim 28 is rejected for the same reasons as claims 7-8 above.

42. Claim 29 is rejected for the same reasons as claim 11 above.

43. Regarding claim 30, Schuermann disclosed the TIRIS reader causing the initialization of the ignition, an engine control module (See Schuermann Col. 8 Paragraph 5).

44. Regarding claim 31, Schuermann clearly depicted the TIRIS reader coupled to a processor for controlling the vehicle settings and ignition initialization (See Schuermann Figure 1 Elements 10, 33, and 34b, and Col. 8 Paragraph 5).

45. Regarding claim 32, Schuermann disclosed that the vehicle performance and maximum speed (operational parameters) were associated with the key transponder (See Schuermann Col. 8 Paragraph 1). Schuermann also disclosed that the key transmitted access codes to the reader, which the reader verified, and then the settings were initialized (See Schuermann Col. 8 Paragraph 5). Schuermann further disclosed that the Reader and key communicated via RF transmissions, which falls within the scope of telematics (See Schuermann Col. 8 Paragraph 5).

46. Claim 33 is rejected for the same reasons as claim 24 above.

47. Regarding claim 34, Schuermann disclosed storing toll credit limits and charge deduction and billing information from a parking toll station (See Schuermann Col. 9 Paragraph 7).

48. Regarding claim 35, Schuermann disclosed that the controller identified each transponder by the data stored on each (See Schuermann Col. 8 Paragraph 2). Therefore, the controller must have used the data stored in the transponder, as discussed for claim 34 above, for identification purposes. Schuermann further disclosed that the controller interrogated the transponders (See Schuermann Col 9 Paragraph 6) and that the TIRIS reader was used for communications between the transponders and the controller (See Schuermann Col. 3 Paragraph 3). It is therefore inherent that the TIRIS reader must have retrieved the data from the transponder and then submitted it to the interrogating controller.

49. Claim 36 is rejected for the same reasons as claim 24 and further due to the obvious nature of the claim. That is, it would have been obvious to the ordinary person skilled in the art to not allow re-authentication if the rule set did not allow re-authentication and to allow it if the rule set allowed it. This would have been obvious because the ordinary person skilled in the art would have been motivated to follow the rules of each rule set.

50. Claim 44 and 46 are rejected for the same reasons as claim 25 above, as applied to claim 40 above.

51. Regarding claim 45, Schuermann disclosed the operational limitations being enabled according to the capabilities of the key holder. It was inherent that the combination of Schuermann and Treharne be able to provide a new user with full operational privileges if the holder of the new key did not require limitations.

52. Claim 52 recites program instructions executable on a first computational device for authenticating an encoding device coupled to the central authority. Schuermann disclosed the controller verifying the access codes received from the encoder of the transponder (See Schuermann Col. 8 Paragraph 5). It was inherent that the controller had the necessary program instructions to carry out this functionality.

Claim 52 further recites second program instructions for authorizing a request sent via the network from the encoding device for programming the access device with one of the tags. Treharne disclosed the request for programming the new key, authorizing the request, and programming the new key as a valid entry key (See Treharne Col. 3 Paragraph 1). Because the request is made by an attempt to use the new transponder, it was inherent that the new transponder sent the request through its RF encoder. It was also inherent that the controller of Schuermann was provided the necessary program instructions to enable this functionality.

Claim 52 further recites third program instructions executable on the first computational device for authorizing a request from the encoding device for programming an authentication device with a plurality of identification tags and associated rule sets, wherein each identification tag and rule set pair establishes a level of operation privileges for a user (See rejection of claims 7, 8 and 9 above, and further it was inherent that the controller of Schuermann was provided the necessary program instructions to enable this functionality).

Claim 52 further recites fourth program instructions executable on a second computational device for providing the corresponding level of operation privileges to the user if the identification tag programmed in the access device matches with at least one of the plurality of identification tags programmed in the authentication device (See rejection of claim 11 above, and further it was inherent that the TIRIS reader of Schuermann was provided the necessary program instructions to enable this functionality).

Claim 52 further recites that the fourth program instructions are further executable for providing a default level of operation privileges to the user if the identification tag programmed in the access device does not match with at least one of the plurality of identification tags programmed in the authentication device (See rejection of claim 43 above, and further it was inherent that the reader of Schuermann was provided the necessary program instructions to enable this functionality).

Claim 52 further recites fifth program instructions executable on the second computational device for bypassing the corresponding level of operation privileges and providing a dissimilar level of operation privileges (See rejection of claim 37 above, it was inherent that the controller and reader of Schuermann were provided the necessary program instructions to enable this functionality.

53. Claim 57 is rejected for the same reasons as claim 25 and further because it was inherent that the controller and reader of Schuermann were provided the necessary program instructions to enable this functionality.

54. Claim 58 recites program instructions executable on a first computational device for authenticating an encoding device coupled to the central authority. Schuermann disclosed the controller verifying the access codes received from the encoder of the transponder (See Schuermann Col. 8 Paragraph 5). It was inherent that the controller had the necessary program instructions to carry out this functionality.

Claim 58 further recites second program instructions authorizing a request sent via the network authenticating a first access device, which contains an identification tag associated with operational privileges of the user. Schuermann disclosed the TIRIS reader/writer re-authenticating the transponders on a regular basis, including the access device (Element 22) (See Schuermann Col. 8 Paragraph 4). Schuermann further disclosed the transponder sending its identification codes (request for authentication) to the TIRIS reader controller and the controller receiving and verifying the codes (determining authorization) (See Schuermann Col 8. Paragraph 5 and Element 10). Schuermann also disclosed transponder (Element 22) containing programmed tags, as discussed for claim 1 above. It was inherent that the controller had the necessary program instructions to carry out this functionality.

Claim 58 further recites that the second program instructions are further executable to retrieve data from the access device, wherein the data comprises operational metrics of the user for the corresponding level of operation privileges provided to the user by the first access device (See the rejection of claims 34-35 above, and further it was inherent that the controller had the necessary program instructions to carry out this functionality).

55. Claim 58 further recites that the second program instructions are further executable for authorizing the authentication request if the data conforms to the level of eligibility for authentication as established for the corresponding level of operation privileges (See the rejection of claim 36 above, and further it was inherent that the controller had the necessary program instructions to carry out this functionality).

Claim 58 further recites third program instructions executable on the computational device for authenticating a second access device to the central authority (See the rejection of claim 25 above and further it was inherent that the controller had the necessary program instructions to carry out this functionality).

Claim 58 further recites that the third program instructions are further executable for authorizing the authentication request if the second access device is configured as a master to the first access device (See the rejection of claim 25 above, and further because the valid key, See Treharne Figure 3 Step 54, falls within the scope of a master to the new key, wherein the new key is the is the first access device of claim 58 above).

Response to Arguments

56. Applicant's arguments filed 8/27/2004 have been fully considered but they are not persuasive. Applicant traverses primarily that:

I. The cited prior art does not teach the central authority being connected to the Internet.

II. The cited prior art does not teach the first, second, and third devices being connected via the Internet.

III. The cited prior art does not teach bypassing a level of operation privileges of an identification tag and rule set pair by disabling future accesses to the identification tag on the access device.

IV. The cited prior art does not teach providing a default level of operation privileges to a user if a matching tag is not found.

V. The cited prior art does not teach a second access device authorizing an authentication request if the second device is configured as a master of the first.

57. Applicant's arguments I, with respect to claims 1, 7, 13, and 19 have been considered but are moot in view of the new ground(s) of rejection. As shown in the rejection of claim 7 above,

when the controller is authorizing the credit transaction, it is in a network connection with the tollbooth, which is also in a network connection with the Internet. These two connections place the controller in connection with the Internet.

58. Applicant's arguments II, with respect to claim 1, have been considered but are moot in view of the new ground(s) of rejection.

59. Regarding applicant's arguments III, with respect to claims 25, and 52, the examiner does not find the arguments persuasive. Applicant failed to recognize the combination of Schuermann and Treharne, but instead focused only on Schuermann alone. As discussed above, in this combination, the newly programmed key would have received a new level of operating parameters. This new level was the level of the first, authenticated, key. Therefore, the original operating parameters were bypassed, and a dissimilar level of operation parameters were provided to the user of the new tag. Furthermore, in this combination, because the tag was written to the transponder, as disclosed by Schuermann, and the controller identified the transponder by this tag, it was inherent that the new tag granting privileges replaced the old tag on the transponder. Therefore, access to the old tag was disabled.

60. Regarding applicant's arguments IV, with respect to claims 40 and 52, the examiner does not find the arguments persuasive. As discussed above, Schuermann disclosed that if the tag in a key did not match the proper identification code, the engine would either not start, or would not continue to run. Although applicant feels that this does not constitute a default level of operating privileges, the examiner disagrees. In this case, although the privileges were not high, they were still a default level. This is especially evident in that if the engine was running when the

controller detected that a proper code was not present, the engine would revert to the default level of not running. Therefore, Schuermann did in fact disclose this limitation.

61. Regarding applicant's argument V, with regards to claim 58, the examiner does not find the arguments persuasive. Simply because Schuermann and Treharne did not use the specific terms master key and normal (or slave) key, does not mean that they are not in fact the same thing. In the teachings of Treharne, as discussed above, a first key is authenticated in order to control the programming of a second key. This first key, is acting as a master key, and the second key is acting as a slave key. According to Microsoft Press Computer Dictionary, Third Edition, master/slave arrangement is defined as "a system in which one device, called the master, controls another device, called the slave. Clearly, in the combination of Schuermann and Treharne as presented above, the first key controls the programming of the second key. Therefore, the first key is a master key and the second key is a slave key.

Conclusion

62. Claims 1-3, 5, 7-11, 13-17, 19-20, 22-25, 27-36, 40, 44-46, 52, and 57-58 have been rejected.

63. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Schuermann et al. (U.S. Patent Number 5,552,789) disclosed a transponder comprising an interrogator for reading and writing to the transponder via RF communications.

b. Moseley (U.S. Patent Number 5,193,114) disclosed a method for authenticating a smart card and encrypting the communications with the smart card.

c. Beigel et al. (U.S. Patent Number 5,257,011) disclosed a method for altering the data of a transponder.

d. Boyles (U.S. Patent Number 5,323,140) disclosed a method for bypassing an anti-theft system in a vehicle involving a button and an ignition key.

e. Drexler et al. (U.S. Patent Number 5,457,747) disclosed a method for authorizing smart card usage in order to gain privileges.

f. Murphy (U.S. Patent Number 5,712,625) disclosed a method of adaptation to a user by identification key transmitter.

g. Brinkmeyer et al. (U.S. Patent Number 5,708,712) disclosed an electronic key for storing an identification code, which has been encrypted on the basis of a one-way function.

h. Deo et al. (U.S. Patent Number 5,721,781) disclosed a smart card authentication system involving certificates.

i. Ohashi et al. (U.S. Patent Number 5,761,309) disclosed a smart card authentication method involving both master and slave authentication centers.

j. Brinkmeyer et al. (U.S. Patent Number 5,774,550) disclosed a method of authorization and synchronization of a smart card.

k. Lenart et al. (U.S. Patent Number 5,880,679) disclosed a method of enabling a vehicle from a remote location.

64. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
1/26/2004

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER